UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/731,509	12/07/2000	Thomas Schaeck	DE919990082	1249

46369 7590 01/29/2008

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
01/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/731,509	SCHAECK ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-20,22-36,38-43 and 45-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-20,22-36,38-43 and 45-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In communications filed on 11/20/2007, applicant amends claims 16, 19, 20, 28, 32-36, 40-43, and 47. The following claims 16-20, 22-36, 38-43, and 45-47 are presented for examination.

1.1 Applicant's remarks, filed on 11/20/2007, with respect to the art rejection of the claims have been fully considered but they are not persuasive. Regarding claim 16, Applicant argues that Rikuna does not disclose one of the identifiers is from the card because the only thing coming from the terminal is the key for decrypting the EN-PAN which is not the thing being compared to the PAN. Examiner disagrees with applicant's interpretation because that the key is not the thing being compared, rather it's the decrypted PAN coming from the terminal that is being compared with the PAN from the card (see column 8, lines 10-23), and therefore meets the claimed limitation. Applicant also argues that Rikuna does not disclose without a holder of the card providing information as amended. Examiner respectfully disagrees because the claim as amended is still not patentably distinct from Rikuna. The claim recites the verification is performed without a holder of the card providing information by providing another identifier to the card from the at least one device for comparing. In other words the claim has been amended to recite that the information for verification is not provided by the user but by at least one device. As interpreted by Examiner Rikuna discloses since the PIN is preliminary stored into the second card, and then transferred to the terminal, the user does not have to be present nor key

input the PIN data for verifying the PIN number by the card, all the user has to do is to hand his own user card and the remote PIN card and the verification by the user card can take place at any time using only the user card because the PIN number is stored in the remote PIN card and subsequently in the terminal (see column 8, lines 34-36 and column 8, lines 58-65 and column 3, lines 9-12). In response to applicant's arguments that requiring PIN entry only when the amount of transaction exceeds a preselected floor limit cannot be interpreted as a trusted association, Nakamura discloses in eliminating the PIN validation, the user of the card is assumed to be the rightful possessor of the card and a restriction is imposed to enter PIN to prevent use of a fraudulently issued card and unauthorized terminal (column 5, line 64 through column 6, line 16). Therefore, applicant has not overcome the rejection and the claims remain rejected. The rejection of the dependent claims not argued by Applicant can still be applied in this Office action.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 41-43 and 45-47 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 41 and 47 recite "an article of manufacture comprising... and further discloses at least one computer usable medium having computer

readable program code logic to control card holder verification the computer readable program code logic comprising check logic... and logic..." It appears that the computer usable medium recited in the claims are not described in the specification (see page 17) as including a tangible medium in a manner which enables it to act as a computer component to realize the computer program's functionality. The claim does not appear to fall within a statutory category and therefore is non-statutory under 35 U.S.C. 101.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 16-20, 22, 25, 28-36, 38-43, and 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 4,752,678 to **Rikuna** in view of US Patent 5,917,168 to **Nakamura et al**.

As per claim 16, **Rikuna** substantially discloses a method for controlling card holder verification comprising: determining/checking presence of a trusted association between the

terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison section 63 with identifiers (decrypted PAN) stored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the checking comprises comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device.* **Rikuna** discloses when the first identifiers coincide (i.e. card is valid), performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of (*if the checking indicates the presence of the trusted association then performing card holder verification separate from the comparing);* **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column 8, lines 58-65, and column 3, lines 9-12) that meets the recitation of *performing card holder verification separate from the comparing using the card and without a holder of the card providing information by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored on the card that is different from the first identifier*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key

inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45) that meets the recitation of *otherwise, then involving the holder of the card in performing card holder verification by the card.* **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67) but is silent about performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the terminal, and the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna** .

Nakamura et al in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card.* **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued

card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 17, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the at least one device is located in a trusted environment (see column 3, lines 15-23).

As per claim 18, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the card comprises a chipcard (see column 1, lines 25-30).

As per claim 19, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the performing card holder verification without a holder of the card providing information comprises performing card holder verification hidden from the holder of the card (see column 8, lines 38-45 and column 8, lines 58-65).

As per claim 20, the references as combined above disclose the claimed method of claim 19. **Rikuna** discloses wherein the performing card holder verification hidden from the holder of the card comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without the holder of the card providing the personal identification number (see column 8, lines 38-45 and column 8, lines 58-65).

As per claim 22, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses wherein the comparing comprises comparing a card identifier stored on the card with one or more card identifiers stored in the device (see column 8, lines 5-27).

As per claim 25, the references as combined above disclose the claimed method of claim 16. **Rikuna** discloses a card storing attribute data including account number, merchant identification code and terminal identification code (device identifier) (see column 4, lines 21-26) and disclose an exemplary embodiment for checking some of the attribute data such as account number, merchant identification code (see column 7, line 40 through column 9, line 23). **Rikuna** is silent about checking terminal identification code meaning comparing an identifier of the device with one or more device identifiers stored on the card. However, it would only require routine skill in the art and design choice to reproduce the process disclosed by **Rikuna** of comparing the other attribute data or identifiers such as account number, merchant identification code, PIN, etc. and use it to compare the terminal identification code (device identifier). One of ordinary skill in the art would have recognized the advantage of comparing terminal identification code so as to determine if the IC card terminal is authorized or not as suggested by **Rikuna** (see column 1, lines 34-36) and as suggested by **Nakamura et al** who discloses mutual authentication for preventing use of unauthorized terminal (see column 6, lines 11-24).

As per claim 28, the references as combined above disclose the claimed method of claim 16, **Rikuna** discloses wherein the performing card holder verification without a holder of the card providing information comprises automatically obtaining a personal identification number

of the holder of the card and verifying the personal identification number without requesting information from the holder of the card (see column 8, lines 5-27, column 8, lines 58-65, and column 3, lines 9-12) and wherein the involving the holder of the card comprises requesting the holder of the card to enter the personal identification number (see column 3, lines 21-31).

As per claim 29, the references as combined above disclose further comprising associating the at least one device and the card (see **Rikuna,** column 3, lines 15-23 and column 7, lines 40-52).

As per claim 30, the references as combined above disclose further comprising controlling the association between a device of the at least one device and the card (see **Rikuna,** column 3, lines 15-23 and column 7, lines 40-52).

As per claim 31, the references as combined above disclose wherein the controlling comprises using a network connectable to the device (see **Nakamura et al**, column 5, lines 40-52).

As per claim 32, the references as combined above disclose the claimed method of claim 16, wherein the checking is between at least one device and a plurality of cards and where in the performing card holder verification without a holder of the card providing information is for a plurality of holders (see **Rikuna,** column 2, line 65 through column 3, line 12).

As per claim 33, **Rikuna** substantially discloses a method for performing card holder verification said method comprising: determining/checking presence of a trusted association between the terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison section 63 with identifiers (decrypted PAN) stored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the checking comprises comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device*. **Rikuna** discloses when the first identifiers coincide (i.e. card is valid), performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of *performing card holder verification by the card separate from and based on the checking*. **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column 8, lines 58-65, and column 3, lines 9-12) that meets the recitation of *if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card different from the first identifier is automatically provided to the card from the at least one device and verified using the card without the holder of the card providing information*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which

could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45) that meets the recitation of *otherwise, then the holder of the card is requested to enter the personal identification number to verify the holder of the card via the card comparing the personal identification numbered entered to a second identifier stored on the card.* **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67) but is silent about performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the terminal, and the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna**.

Nakamura et al in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card.* **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made

to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 34, **Rikuna** substantially discloses a system for performing card holder verification said system comprising: determining/checking presence of a trusted association between the terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison section 63 with identifiers (decrypted PAN) stored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *means for checking the presence of a trusted association between at least one device and a card usable with the at least one device, wherein the means for checking comprises means for comparing by one of the card and the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device a first identifier stored on the card with one or more identifiers stored in the at least one device*. **Rikuna** discloses when the first identifiers coincide (i.e. card is valid), performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of *means for performing card holder verification separate from the comparing using the card.* **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and

for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column 8, lines 58-65) that meets the recitation of *means for performing card holder verification separate from the comparing using the card and without a holder of the card providing information by providing another identifier to the card from the at least one device for comparing by the card to a second identifier stored on the card that is different from the first identifier if the checking indicates the presence of the trusted association*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45, and column 3, lines 9-12) that meets the recitation of *otherwise, then means for involving the holder of the card in performing card holder verification by the card.* **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67) but is silent about performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the terminal, and the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna**.

Nakamura et al in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to

prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card.* **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 35, the references as combined above disclose the claimed system of claim 34, **Rikuna** discloses wherein the means for performing card holder verification without a holder of the card providing information involvement comprises means for performing card holder verification hidden from the holder of the card (see column 8, lines 38-45).

As per claim 36, the references as combined above disclose the claimed system of claim 35, wherein the means for performing card holder verification hidden from the holder of the card comprises means for automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without the holder of the card providing the personal identification number (see **Rikuna,** column 8, lines 38-45).

As per claim 38, **Rikuna** discloses the claimed system of claim 34, wherein the means for comparing comprises means for comparing a card identifier stored on the card with one or more card identifiers stored in the device (see **Rikuna,** column 8, lines 5-27).

As per claim 39, **Rikuna** discloses the claimed system of claim 34, wherein the means for comparing comprises (comparison section 40) that meets the recitation of means for comparing an identifier of the device with one or more device identifiers stored on the card (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 40, **Rikuna** substantially discloses a system of performing card holder verification, said system comprising at least one processor (see figure 3) to perform card holder verification based on determining/checking presence of a trusted association between the terminal 12 and the card 11 by comparing a first identifier (i.e. PAN primary account number) stored in card 21 by the comparison section 63 with identifiers (decrypted PAN) tored in terminal 12 (see column 8, lines 5-27) that meets the recitation of *at least one processor on the card to perform card holder verification based on whether a trusted association exists between at least one device and a card usable with the at least one device, and to compare a first identifier stored on the card with one or more identifiers stored in the at least one device.* **Rikuna** discloses when the first identifiers coincide (i.e. card valid) performing cardholder verification separate from the comparing above (see column 8, lines 24-30) that meets the recitation of (*if the checking indicates the presence of the trusted association then performing*

card holder verification separate from the comparing); **Rikuna** further discloses cardholder verification is performed separate from the first comparing above by comparing the PIN using the card (comparison section 40) and without a holder of the card providing the PIN (the holder of the card hands in the card for verification) the PIN is provided from the terminal 12 to the card and for comparing by the card to the PIN stored in the card that is different from the PAN (first identifier) (see column 8, lines 38-45 and column 8, lines 58-65, and column 3, lines 9-12) that meets the recitation of *if the checking indicates the presence of the trusted association, then a personal identification number of the holder of the card different from the first identifier of the holder of the card is automatically provided to the card from the at least one device and verified separate from the compare using the card without the holder of the card providing information*; **Rikuna** also discloses if there is indication that an identifier is not transferred to the terminal (which could be interpreted as no trusted association) then involving the cardholder in performing cardholder verification by directly key inputs the PIN data by the card as in step B15 (see column 9, lines 26-37 and column 8, lines 38-45) that meets the recitation of *otherwise, then the holder of the card is requested to enter the personal identification number to verify the holder of the card via the card comparing the personal identification numbered entered to a second identifier stored on the card.* **Rikuna** suggests different scenarios in verifying the holder of the card by the card when authentication fails (see column 9, lines 25-67) but is silent about performing the verification when *the checking indicates no trusted association* (i.e. card invalid). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to add the feedback mechanism disclosed by **Rikuna** of verifying the cardholder in case of any authentication failure due to the card, the terminal, and

the account itself (including trusted association) for the predictable result of ensuring that the holder of the card is authentic as suggested by **Rikuna**.

Nakamura et al in an analogous art discloses automatic debit operation without PIN entry (see column 5, line 39 through column 6, line 7) and further discloses another option is to require PIN entry only when the amount of the transaction exceeds a preselected floor limit to prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal (see column 6, lines 11-24) that meets the recitation of *if the checking indicates no trusted association then involving the holder of the card in performing card holder verification by the card.* **Nakamura et al** adds a mutual authentication then would prevent use of a fraudulent issued card and use of unauthorized terminal (see column 6, lines 11-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Rikuna** to involve the holder of the card in performing card holder verification if the checking indicates no trusted association because one of ordinary skill in the art would have recognized the advantages that doing so would prevent use of a fraudulent issued card to complete a transaction and use of unauthorized terminal as suggested by **Nakamura et al**.

As per claim 41, **Rikuna** discloses a method to control card holder verification that can be implemented in hardware and software that meets the recitation of an article of manufacture comprising at least one computer usable medium having computer readable program code logic to control card holder verification. Claim 41 recites similar limitations as claim 16 except for

incorporating the claimed method into a computer program. Therefore, claim 41 is rejected on the same rationale as the rejection of claim 16.

As per claims 42, 43, 45, and 46,these claims recite the same limitations as claims 19, 20, 22, and 25 respectively except for incorporating the claimed method into a computer program. Therefore, these claims are rejected on the same rationale as the rejection of claims 19, 20, 22, and 25.

As per claim 47, **Rikuna** discloses a method to control card holder verification that can be implemented in hardware and software that meets the recitation of an article of manufacture comprising at least one computer usable medium having computer readable program code logic to control card holder verification. Claim 47 recites similar limitations as claim 33 except for incorporating the claimed method into a computer program. Therefore, claim 47 is rejected on the same rationale as the rejection of claim 33.

4. **Claims 23-24 and 26-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 4,752,678 to **Rikuna** in view of US Patent 5,917,168 to **Nakamura et al** as applied to claims 16, 22, and 25 and further in view of US Patent 6,473,500 to **Risafi et al.**

As per claim 23, both references disclose the claimed method of claims 16 and 22. **Rikuna** does not explicitly disclose replacing the personal identification number which is a common practice in the art. **Risafi et al** in an analogous art discloses wherein the card identifier

is associated with a personal identification number usable in card holder verification and said method further comprises replacing the personal identification number with another personal identification number (see column 4, lines 17-47). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to allow the cardholder to select and change the PIN at any time as taught by **Risafi et al** because it would be advantageous to have the user select a PIN that is easily remembered (see column 3, lines 35-44).

As per claim 24, the references as combined above disclose the claimed method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprising erasing the association between the card identifier and the personal identification number (see **Risafi et al,** column 4, lines 17-47). Therefore, this claim is rejected on the same rationale as the rejection of claim 23 above.

As per claim 26, the references as combined above disclose the claimed method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, (see **Rikuna** column 4, lines 21-27) and said method further comprises replacing the personal identification number with another personal identification number (see **Risafi et al,** column 4, lines 17-47). Therefore, this claim is rejected on the same rationale as the rejection of claim 23 above.

As per claim 27, the references as combined above disclose the claimed method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification (see **Rikuna** column 4, lines 21-27), and said method further comprising erasing the association between the card identifier and the personal identification (see **Risafi et al,** column 4, lines 17-47). Therefore, this claim is rejected on the same rationale as the rejection of claim 23 above.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Carl Colin
Patent Examiner, Art Unit 2136
January 23, 2008